REMARKS/ARGUMENTS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application fail to comply with 35 USC § 112, first paragraph, and that none of the claims now pending in the application are obvious under the provisions of 35 USC § 103 (a). Thus, the Applicants believe that all of these claims are now in allowable form.

Reexamination and reconsideration of the application are respectfully requested. If, however, the Examiner believes that there are any unresolved issues in any of the claims now pending in the application, the Examiner should telephone Ms. Janet M. Skafar, Esq. at telephone number (650) 988-0655 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Status of Claims

Claims 1, 7, 15, 23, 29, and 37 have been amended. Claims 13, 14, 21, 22, 35, 36, 43 and 44 have been canceled. Claims 45-47 have been added. Claims 1-12, 15-20, 23-34, 37-42 and 45-47 remain pending in this application.

Claim Rejections under 35 U.S.C. § 112

Claims 1-12, 15-20, 23-34 and 37-42 are rejected under 35 USC § 112, first paragraph, as failing to comply with the written description requirement. The rejection asserts that the specification fails to provide adequate support for the decryption of a data element where the previous data element transmission failed. Applicants respectfully disagree.

Applicants believe that support can be found in the specification as follows. Page 19, lines 7 to 10 teach: Third, if an unreliable channel is used, the data decryption method 504 requires a way to recover the state, "s," 604 in order to decrypt the data 103 that follows the transmission loss. That is, the data decryption method 504 includes state recoverability information in the form of the state, "s," 604.

Page 20, lines 13 to 24 teach: Recoverability via use of a state enables decryption to continue without re-transmitting a buffer if it is lost. Therefore, the present invention transmits the saved state, "s," 604 to the client computer system 150 (as shown in Figure 1). The purpose of including the saved state, "s," 604 in the same transmission as the encrypted payload buffer, "B," 602 is to ensure that decryption is successful even if an individual payload buffer, "B," 602 is lost. Those skilled in the art will appreciate that the saved state, "s," 604 is a value that represents the state at the time immediately preceding the encryption of the payload buffer "B," 602. It will be appreciated that the process of encrypting a buffer changes the state. When any data element 103 within the payload buffer "B," 602 is corrupt the entire payload buffer "B," 602 is considered corrupt. The output of encryption is the input for the decryption operation.

Page 22, lines 1 to 12 teach: The present invention detects if a payload buffer, "B," 602 was lost during transmission over the input channel, "F," 608 by determining if the input channel, "F," 610 is unreliable, as shown element 566. It will be recognized by those skilled in the art that the ability to detect the loss of a data transmission packet 115 (as shown in Figure 1) over an unreliable channel can be accomplished by techniques known in the art. For example, data transmission packet 115 loss can be determined by including a sequence number with each data transmission packet 115 and comparing sequence numbers of successive data transmission packets 115 to assess transmission continuity. If the input channel, "F," 608 is reliable, the operation moves directly to element 572. Alternately, if the input channel, "F," 608 is an unreliable channel, as shown in element 566, the present invention extracts the state, "s," 604 from the payload buffer, "B," 602 as shown in element 568.

Page 22, lines 14 to 17 teach: Further, if there is a data transmission packet 115 loss, as shown in element 570, the present invention uses the saved state, "s," 604 to recover the state of the encrypted information, as shown in element 571.

Page 23, lines 8 to 9 teach: The payload buffer, "B" 602 is a collection of data elements that is transmitted between computer systems.

Page 23, lines 18 to 21 teach: For example, when the output channel is an Internet Protocol Socket operating over an Ethernet connection, an efficient size for the payload buffer, "p," 606 is the size that can be transported in a single Ethernet data transmission packet 115 (as shown in Figure 1).

Hence, the specification describes that the loss of a packet can be detected using a sequence number, and comparing sequence numbers of successive data transmission packets to assess transmission continuity. Thus, the specification discloses successive packets which implies that a packet will follow another packet. Therefore the specification inherently discloses the existence of a packet and a previous packet, and also inherently discloses the existence of a previous packet and a subsequent packet. Referring to Fig. 5C, element 564 reads data in payload buffer "B" from channel "F". Element 566 determines whether "F" is reliable. If not, element 568 extracts the state "s" from the payload buffer "B". Element 570 determines whether a data transmission packet was lost. For example, the specification teaches that it can be determined whether a data transmission packet was lost by comparing sequence numbers of successive data transmission packets. For example, assume that the current packet has a sequence number of i. If the previous packet has a sequence number of i-1, then no data transmission packet was lost. If the previous consecutive data transmission packet has a sequence number of i-2, then the data transmission packet with sequence number of i-1 was lost.

If element 570 determines that a data transmission packet was lost, element 571 uses "s" (extracted in element 568) to recover the state. Element 572 performs decryption in the reverse order of encryption. If step 562 determines that decrypted data processing is not complete, element 562 proceeds to element 564 to continue to read data in the payload buffer.

Therefore, if a previous packet is lost during transmission, there is a transmission failure of the previous packet. Therefore, the state "s" which is included in the transmission of a subsequent packet is used for decryption. Because a packet comprises the payload buffer and the payload buffer comprises data elements, if a previous packet is lost, any data elements in that previous packet are lost, that is, a previous data element is lost, and there is a transmission failure of the previous data element. The subsequent packet also comprises data elements and an ecryption state. Therefore, Applicants respectfully submit that there is support for the recitation: "in response to said determining said transmission of said previous encrypted data element failed, decrypting said encrypted data element with said static key, said encryption state transmitted with said encrypted data element, and said dynamic key without retransmission of said previous encrypted data element."

Claim Rejections under 35 U.S.C. § 103(a)

Claims 1-5, 7-10, 12, 15-18, 20-27, 29-32, 34, 37-40 and 42 are rejected as being unpatentable over Mitty et al. US Patent No. 6,145,079 ("Mitty") in view of Shimomura et al U.S. Patent No. 6,145,079 ("Shimomura") and Liechti et al U.S. Patent No. 5,715,164 (Liechti). The rejection asserts that Mitty fails to teach that in response to a transmission failure of said data element, decryption of said data element being recovered without retransmission of said data element, decryption of said data element being recovered without retransmission of data and the use of encryption states. The rejection asserts that Liechti teaches an encryption state being associated with said data element being statically encrypted with said static key (column, 8, lines 17-29, key and value which is a function of a previous block). The rejection also asserts that Shimomura teaches that in response to a transmission failure of said data element, decryption of said data element being recovered without retransmission of data (Shimomura, column 14, lines 5-15) thus allowing decryption of a subsequent block to take place even if there was a transmission failure. The rejection contends that at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Shimomura's correction method with Mitty's secure transaction system because it offers the advantage of ensuring that received data is not lost or altered (Shimomura,

column 14, lines 5-15) and helps hide repeated patterns in encrypted data which helps defeat attempts at cryptanalysis (Liechti, column 1 lines 49-59).

Claims 1, 7, 15, 23, 29 and 37 have been amended to more particularly point of the invention. In addition, Claims 1 and 23 have been amended to more particularly point out the invention by including a distinguishing recitation of Claim 7.

Applicants respectfully submit that the combination of Mitty, Liechti and Shimomura, explicitly or implicitly, does not teach all the recitations of Claims 1-5, 7-10, 12, 15-18, 20-27, 29-32, 34, 37-40 and 42. The rejection will be discussed with respect to independent Claim 7.

Applicants respectfully submit that the recitation of Claim 7 of "transmitting said encrypted data element with said encryption state to a receiving computer system" is not taught, alone or in combination, explicitly or implicitly, by Mitty, Liechti and Shimomura. The rejection asserts that Liechti teaches an encryption state being associated with said data element being statically encrypted with said static key. Even assuming that Liechti teaches an encryption state being associated with said data element being statically encrypted with said static key, Applicants respectfully submit that Liechti does not teach "transmitting said encrypted data element with said encryption state to a receiving computer system". In addition, because the encrypted data element is not transmitted with the encryption state, decryption cannot be performed using the encryption state transmitted with the encrypted data element.

Claim 7 has the following recitation: "decrypting said encrypted data element with said static key, said encryption state transmitted with said encrypted data element, and said dynamic key without retransmission of said previous encrypted data element." The result of this recitation is that if a previous data element is lost, the claimed invention decrypts the data element, which is inherently subsequent to the data element that is lost, using the encryption state transmitted with the data element. Using the claimed invention, the lost data element does not need to be retransmitted or recovered to decrypt a subsequent data element. That it is not necessary to recover the previous data element is contrary to the motivation of ensuring that received data is not lost or altered. Therefore,

one of ordinary skill in the art would not utilize Shimomura's correction method with Mitty's secure transaction system.

For the foregoing reasons, Applicants submit that neither Mitty nor Shimomura nor Liechti, alone or in combination, explicitly or implicitly, teaches all the recitations of Claim 7. Therefore, Applicants respectfully submit that Claim 7 is patentable. Claims 8-10, 12 depend from Claim 7 and are patentable for the same reasons as Claim 7.

Claim 1 has similar distinguishing limitations as Claim 7; therefore Applicants respectfully submit that Claim 1 is patentable for the same reasons as Claim 7. Claims 2-5 depend from Claim 1, and are patentable for the same reasons as Claim 1.

Independent Claims 15, 23 and 37 contain similar distinguishing recitations as Claim 7 and are patentable for the same reasons as Claim 7. Claims 16-18, 20; 24-27; and 38-40, 42 depend from Claims 15, 23 and 37, and are patentable for the same reasons as Claims 15, 23 and 37, respectively.

Claim 29

Claim 29 has similar distinguishing recitations as Claim 7 and Applicants respectfully submit that Claim 29 is patentable for the same reasons as Claim 7.

Claim 29 also recites that "wherein said previous one of said dynamic-static data element chunks associated with said failed transmission is not recovered.

The Response to Arguments contends that "Claim 1 only provides that no retransmission is attempted after a transmission failure and in no way states that recovery does not occur. However, Claim 29 recites that "wherein said previous one of said dynamic-static data element chunks associated with said failed transmission is not recovered". Applicants respectfully submit that the flowchart of Figure 5C and the above discussion with respect to the rejection under 35 USC 112, also provides support for this recitation.

Applicants submit that neither Mitty nor Liechti nor Shimomura, alone or in combination, explicitly or implicitly, have such a teaching; therefore, for the foregoing additional reasons, Applicants respectfully submit that Claim 29 is not obvious.

Claims 30-32 and 34 depend from Claim 29, and Applicants respectfully submit that Claims 30-32 and 34 are patentable for the same reasons as Claim 29.

Claims 6, 11, 19, 28, 33 and 41

Claims 6, 11, 19, 28, 33 and 41 are rejected as being unpatentable over Mitty in view of Shimomura and Liechti, and further in view of Bailey III US Patent No. 5,659,614 ("Bailey").

Claims 6, 11, 19, 28, 33 and 41 are dependent on independent Claims 1, 7, 15, 23, 29 and 37, respectively. For all the reasons put forth with respect to independent Claims 1, 7, 15, 23, 29 and 37, Applicants submit that Claims 6, 11, 19, 28, 33 and 41 are not obvious over Mitty, Liechti and Shimomura. Applicants also submit that Bailey III does not teach all the recitations of Claims 1, 7, 15, 23, 29 and 37.

Bailey is focused on decryption at a backup site and is related to file data, not chunked data, as expressly recited in Claims 23, 29 and 37. Bailey is directed to "A method and system for prioritizing, securing, and reducing the amount of data transmitted and stored during the creation of a backup copy of file data." [Bailey, Abstract]. In contrast, the claimed invention is directed to the accelerated dynamic protection of data. Further, Bailey requires a data security card for additional numbers to serve as keys (Col. 18, lines 30-44) and this technique is not similar the techniques of Applicants' invention. Therefore, one skilled in the art would not look to the Bailey patent to solve the problem of accelerating the dynamic protection of data. Hence, it would not have been obvious to one skilled in the art to use the techniques of Bailey that are focused on backup techniques for file data, for the purpose of rendering obvious Applicants' invention. For the foregoing reasons, Applicants respectfully request that that Claims 6, 11, 19, 28, 33 and 41 be allowed.

New Claims 45-47

New claims 45, 46 and 47 depend from independent claims 1, 7 and 15 and recite an additional distinguishing recitation: "that said data element comprises digital data representing audio and video information."

Conclusion

For the foregoing reasons, Applicants submit that the pending Claims 1-12, 15-20, 23-34, 37-42, and 45-47 are patentable over the art of record.

Applicants therefore respectfully request that the Examiner reconsider all currently outstanding rejections and that they be withdrawn. It is believed that a full and complete response has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this Application, the Examiner is invited to telephone the undersigned at the number provided. Prompt and favorable consideration of this Response is hereby solicited.

Respectfully submitted,

August 18, 2006

Janet M. Skafar, Attorney
Reg. No. 41,315
Correspondence Customer No. 24852
Telephone: (650)988-0655
Facsimile: (408) 463-4827